

REMARKS

Claims 1-5 and 15-18 are pending in the current application. In an office action dated December 28, 2007 ("Office Action"), the Examiner rejected claims 1-5 and 15-18 under 35 U.S.C. §103(a) as being unpatentable over Colligan et al., U.S. Patent No. 6,519,762 ("Colligan") in view of Crumly, U.S. Patent Application Publication No. 20030161475 ("Crumly"). Applicant respectfully traverses these rejections.

Claim 1 recites:

1. A method for preparing an authenticable and verifiable image of a module, the method comprising:
 - receiving a module image;
 - adding to the module image a size and location block;
 - adding to the module image an authentication block including a cryptographically protected module-specific public key and a clear-text version of the module-specific public key to produce an authenticable image; and
 - adding to the authenticable image a verification block that includes a digital signature prepared from the module image.

Thus, claim 1 is directed to an authenticable and verifiable image of a module that includes a size and location block, an authentication block, and a verification block. The authenticable and verifiable image is a single, multi-block entity, as shown in Figure 3 of the current application.

In the Office Action, the Examiner states:

Colligan teaches with respect to claim 1, a method for preparing an authenticable and verifiable image of a module, the method comprising: receiving a module image (see Colligan column 9 lines 34-38); adding to the module image a size and location block (see Colligan column 9 lines 34-38).

Colligan, according to Colligan's abstract, discloses a method for restoring a hard disk drive on a computer system. Applicants' representative can find no reference, in Colligan, to authentication and verification. The cited portion of Colligan reads:

In step 74, a header file is created on the HDD, the header file containing image information and location. In step 76, the files of the

factory downloaded image are copied, in compressed form, to the restoration image on the HDD, sector by sector.

Applicant's representative can find no mention of authenticability and verifiability in the cited passage, or anywhere else in Colligan. Applicant's representative can find no mention of the word "module," or mention of the phrase "image of a module." Applicant's representative can find no occurrence of the word "size," or any term or phrase related to the word "size," in the cited passage. Applicant's representative can find no occurrence of the phrase "size and location block," or anything related to that phrase in the cited passage, or anywhere else in Colligan.

Those even cursorily familiar with computer science well understand that a block is not a header file. The cited passage of Colligan refers to a method for restoring the contents of a hard disk drive. Hard disk drives are generally organized, at the logical level, as a set of files organized into a hierarchically structured file-directory system. The cited portion of Colligan clearly indicates that a header file is first placed on a hard disk drive, after which additional files of a factory downloaded image are copied to the hard disk drive. Thus, the header file is separate and distinct from the files that constitute the factory downloaded image. The current application and current claims are directed, by contrast, to *an authenticable and verifiable module image that includes* a size and location block. As claimed in claim 1, as discussed in the current application beginning on line 17 of page 9, and as shown in Figure 3, the image size, location, and a globally unique identifier are included in a block 302 within a module image 301. In additional elements of claim 1, an authentication block 308 is added to the module image, and a digital signature 314 is prepared from the module image, including the size, location, and globally unique identifier. There is no indication in Colligan of anything being computed from, related to, or associated with the header file that is separately created on a hard disk drive prior to copying of a set of files representing a software image to the hard disk drive. In short, Colligan does not teach that which the Examiner claims Colligan to teach, as can be easily seen by comparing the first four lines of claim 1 to the above-quoted passage of Colligan cited by the Examiner.

The Examiner next states:

Crumly teaches adding to the module image an authentication block including a cryptographically protected module-specific public key (see Crumly paragraph 0025) and a clear-text version of the module-specific public key to produce an authenticable image (see Crumly paragraph 0025 and 0036); and adding to the authenticable image a verification block that includes a digital signature prepared from the module image (see Crumly paragraph 0036).

Crumly does not teach that for which the Examiner cites Crumly as teaching. First, in paragraph [0025], Crumly describes a physical tag that identifies a public key and that may also identify an address to which an encrypted digital image is sent. Crumly states:

The tag may identify a public key by carrying the entire public key, optionally in the form of a digital certificate in which the public key is encrypted with the private key of a trusted authority. Alternatively, the tag may identify the public key by carrying an identifier that allows the sending device to retrieve or read the public key, by identifying a storage location for the public key.

Claim 1 specifically claims that the authentication block includes "a cryptographically protected module-specific public key and a clear-text version of the module-specific public key." The above-quoted, cited passage of Crumly clearly indicates that the public key occurs in the tag either as the public key itself, or as the public in encrypted form, or is stored in a location referenced by the tag. The cited passage does not even remotely suggest that the tag includes both a clear-text version of the public key as well as an encrypted version of the public key. Moreover, Crumly does not teach, mention, or suggest any reason for including "a cryptographically protected module-specific public key and a clear-text version of the module-specific public key" in Crumly's physical tag or in anything else. *The cited passage does not even teach, mention, or suggest that the tag is included in a module image.* Nothing in this passage teaches, mentions, or even remotely suggests that the public key is specific to a module. The Examiner has apparently neglected to properly consider all of the claim language. As discussed in the current application, and as clearly claimed in claim 1, the cryptographically protected public key that is included in the authentication block is module-specific, in other words, created specifically for the module in which it is included. There is nothing in the cited passage of Crumly that suggests that the public key identified by the tag is specifically

associated with a module, or firmware module. Instead, it appears to be associated with a user.

The Examiner cites paragraph 0036 of Crumly as teaching "adding to the authenticable image a verification block that includes a digital signature prepared from the module image." However, as clearly stated by Crumly in paragraph [0036], a sender may optionally send a digital signature of a digital image along with the encrypted image. There is no indication in Crumly that the digital signature is incorporated in, or included in, the digital image or encrypted digital image, and there is absolutely no mention in either paragraph [0025] or [0036] of Crumly that the encrypted image is "an authenticable and verifiable image of the module." Thus, again, Crumly does not teach that for which the Examiner has cited Crumly.

With respect to claim 15, the Examiner relies on the same passages of Colligan and Crumly which, as discussed above, do not teach, mention, or suggest those elements and limitations for which they are cited. For example, the above-quoted passage from Colligan does not once teach, mention, or suggest a globally unique identifier block. Nothing in that passage could possibly be construed to teach, mention, or suggest a globally unique identifier block. Again, there is no mention of size in the cited passage of Colligan. Colligan is not concerned with, and does not teach, mention, or suggest an authenticable and verifiable image of a module, and does not teach mention, or suggest a size and location block within an authenticable and verifiable image of a module. Crumly does not teach, mention, or suggest including both a cryptographically protected version of a public key as well as the clear-text version of the public key together in an authentication block. Crumly explicitly states that a physical tag includes either a public key, or an encrypted version of the public key, or a reference to the public key, but does not teach, mention, or suggest that the physical tag includes both.

The Examiner has provided no rationale for the obviousness rejection, other than what appears to be the rationale (G) from M.P.E.P. §2143. Rationale (G) depends on the cited references teaching or suggesting that for which they are cited. They do not. Therefore, the obviousness rejection clearly fails. Of course, there is

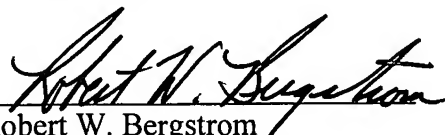
absolutely no teaching, mention, or suggestion for combining Crumly's physical tag with Colligan's hard-disk-drive recovery method. Although the recent *KSR International Co. v. Teleflex, Inc.* decision by the Supreme Court appears to have expanded the various rationales available to an examiner for making an obviousness-type rejection, this decision also indicates that examiners have a much higher obligation for explanation of obviousness-type rejections, as discussed in the first paragraph of M.P.E.P. §2143:

The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in *KSR* noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit.

A single sentence stating that it would have been obvious to include a digital signature of the image, which actually makes little sense in the context of the paragraph in which it is included, offered by the Examiner on lines 5-6 of page 3 of the Office Action, does not even remotely rise to constituting an analysis or any kind of credible reason for attempting to combine two quite dissimilar references to assert obviousness of a claimed invention quite distinct from either reference.

In Applicant's representative's opinion, all of the claims remaining in the current application are clearly allowable. Favorable consideration and a Notice of Allowance are earnestly solicited.

Respectfully submitted,
Chris D. Hyser
Olympic Patent Works PLLC


Robert W. Bergstrom
Registration No. 39,906

Enclosures:
Postcards(2)
Transmittal in duplicate

Olympic Patent Works PLLC
P.O. Box 4277
Seattle, WA 98194-0277
206.621.1933 telephone
206.621.5302 fax